

ON A CONJECTURE OF WAN ABOUT LIMITING NEWTON POLYGONS

YI OUYANG AND JINBANG YANG

ABSTRACT. We show that for a monic polynomial $f(x)$ over a number field K containing a global permutation polynomial of degree > 1 as its composition factor, the Newton Polygon of $f \bmod \mathfrak{p}$ does not converge for \mathfrak{p} passing through all finite places of K . In the rational number field case, our result is the “only if” part of a conjecture of Wan about limiting Newton polygons.

1. INTRODUCTION AND MAIN RESULTS

Let K be a number field and $f(x)$ be a monic polynomial in $K[x]$ of degree $d \geq 1$. For a finite place \mathfrak{p} of K , we let $\mathcal{O}_{\mathfrak{p}}$ be the ring of \mathfrak{p} -adic integers and $k_{\mathfrak{p}}$ be the residue field. Then $k_{\mathfrak{p}}$ is a finite field of $q = q_{\mathfrak{p}} = p^h$ elements for some rational prime $p = p_{\mathfrak{p}}$ and some positive integer $h = h_{\mathfrak{p}}$. Denote by $k_{\mathfrak{p}}^m$ the unique field extension of $k_{\mathfrak{p}}$ of degree m . Denote by Σ_K the set of finite places of K and $\Sigma_K(f)$ the set of places of $\mathfrak{p} \in \Sigma_K$ such that $f(x) \in \mathcal{O}_{\mathfrak{p}}[x]$ and $(d, p) = 1$. Note that $\Sigma_K - \Sigma_K(f)$ is a finite set.

Let \mathfrak{p} be a place in $\Sigma_K(f)$. By modulo \mathfrak{p} , we get the reduction \bar{f} a polynomial over $k_{\mathfrak{p}}$. For a nontrivial character $\chi : \mathbb{F}_p \rightarrow \mu_p$, the L -function

$$L(\bar{f}, \chi, t) = L(\bar{f}/k_{\mathfrak{p}}, \chi, t) = \exp \left(\sum_{m=1}^{\infty} S_m(\bar{f}, \chi) \frac{t^m}{m} \right), \quad (1.1)$$

where $S_m(\bar{f}, \chi)$ is the exponential sum

$$S_m(\bar{f}, \chi) = S_m(\bar{f}/k_{\mathfrak{p}}, \chi) = \sum_{x \in k_{\mathfrak{p}}^m} \chi(\text{Tr}_{k_{\mathfrak{p}}^m/\mathbb{F}_p}(\bar{f}(x))), \quad (1.2)$$

is a polynomial of t of degree $d - 1$ over $\mathbb{Q}_p(\zeta_p)$ by well-known theorems of Dwork-Bombieri-Grothendieck and Adolphson-Sperber [1]. The q -adic Newton polygon $\text{NP}_{\mathfrak{p}}(f)$ of this L -function does not depend on the choice of the nontrivial character χ .

Let $\text{HP}(f)$ be a convex polygon with break points

$$\left\{ (0, 0), \left(1, \frac{1}{d}\right), \left(2, \frac{1}{d} + \frac{2}{d}\right), \dots, \left(d-1, \frac{1}{d} + \frac{2}{d} + \dots + \frac{d-1}{d}\right) \right\},$$

which only depends on the degree of f . Adolphson and Sperber [2] proved that $\text{NP}_{\mathfrak{p}}(f)$ lies above $\text{HP}(f)$ and that $\text{NP}_{\mathfrak{p}}(f) = \text{HP}(f)$ if $p \equiv 1 \pmod{d}$.

Corresponding author: J. Yang. Email: yjb@mail.ustc.edu.cn.

Obviously, there are infinitely many $\mathfrak{p} \in \Sigma_K(f)$ such that $p \equiv 1 \pmod{d}$, thus if $\lim_{\mathfrak{p} \in \Sigma_K} \text{NP}_{\mathfrak{p}}(f)$ exists, then $\lim_{\mathfrak{p} \in \Sigma_K} \text{NP}_{\mathfrak{p}}(f) = \text{HP}(f)$.

Recall that a global permutation polynomial (GPP) over K is a polynomial $P(x) \in K[x]$ such that $x \mapsto \overline{P}(x)$, where \overline{P} is the reduction of P modulo \mathfrak{p} , is a permutation on $k_{\mathfrak{p}}$ for infinitely many places $\mathfrak{p} \in \Sigma_K$.

In 1999, D. Wan proposed a conjecture, whose complete version in [12, Chapter 5] and [3, Conjecture 6.1] is as follows:

Conjecture 1.1 (Wan). *Let f be a non-constant monic polynomial in $\mathbb{Q}[x]$. Then f contains a GPP over \mathbb{Q} of degree > 1 as its composition factor if and only if $\lim_{\mathfrak{p} \in \Sigma_{\mathbb{Q}}} \text{NP}_{\mathfrak{p}}(f)$ does not exist.*

There are little progress on the “if” part, which is much more difficult than the “only if” part. So far, we can only check the “if” part holds for those f of low degrees or of few terms. In this note, we give a proof of the “only if” part of Wan’s conjecture. Moreover, we get the following main result.

Theorem 1.2. *Let f be a non-constant monic polynomial in $K[x]$. If f contains a GPP over K of degree > 1 as its composition factor, then $\lim_{\mathfrak{p} \in \Sigma_K} \text{NP}_{\mathfrak{p}}(f)$ does not exist.*

Remark. If we replace \mathbb{Q} in Conjecture 1.1 by any number field K , then the “if” part does not hold in general. We give an example here. Let ℓ be a prime number greater than 3. Assume $K = \mathbb{Q}(\zeta_{\ell})$ and $f(x) =$ the Dickson polynomial $D_{\ell}(x, 1)$. By Lemma 5.1, f is not a permutation polynomial for all $k_{\mathfrak{p}}$ with $\mathfrak{p} \nmid 3\ell\omega$. Thus f is not a GPP over K . By Lemma 4.1, one can easily check that f is a GPP over \mathbb{Q} . Theorem 1.2 implies that $\lim_{p \in \Sigma_{\mathbb{Q}}} \text{NP}_p(f)$ does not exist. By Proposition 2.6, $\lim_{\mathfrak{p} \in \Sigma_K} \text{NP}_{\mathfrak{p}}(f)$ also does not exist.

2. ZETA FUNCTIONS AND L -FUNCTIONS OF EXPONENTIAL SUMS

In this section, we fix a rational prime p , a positive integer h and let $q = p^h$. Let C be a curve over \mathbb{F}_q . The Zeta function of C

$$Z(C, t) = \exp \left(\sum_{m=1}^{\infty} S_m(C) \frac{t^m}{m} \right) \quad (2.1)$$

is a rational function over \mathbb{Q} , where

$$S_m(C) = \#C(F_{q^m})$$

is the number of \mathbb{F}_{q^m} -rational points of C . If C is smooth and proper, by Weil [11], $Z(C, t)$ is of the form $\frac{P_1(C)}{(1-t)(1-qt)}$, where $P_1(C)$ is a polynomial of t of degree $2g(C)$ over \mathbb{Z} , where $g(C)$ is the genus of C . Denote the q -adic Newton polygon of $P_1(C)$ by $\text{NP}_q^1(C)$.

Let g be a polynomial in $\mathbb{F}_q[x]$ of degree d with $(d, p) = 1$. The fraction field of the integral domain $\mathbb{F}_q[x, y]/(y^p - y - g)$, denoted by L_g , is a Galois extension of $\mathbb{F}_q(x)$, which is the function field of $\mathbb{P}_{\mathbb{F}_q}^1$. So $C(g)$, the normalization of $\mathbb{P}_{\mathbb{F}_q}^1$ in L_g , is a Galois cover of $\mathbb{P}_{\mathbb{F}_q}^1$ with Galois group isomorphic to \mathbb{F}_p . Denote this cover by π . One can check that $\pi^{-1}(\infty)$ is a one-point-set. The complement U of $\pi^{-1}(\infty)$ in $C(g)$ is $\text{Spec}(\mathbb{F}_q[x, y]/(y^p - y - g))$.

In the following we identify (x_0, y_0) with the $\overline{\mathbb{F}_q}$ -point $(x - x_0, y - y_0)$ of $U_{\overline{\mathbb{F}_q}}$ and identify x_0 with the $\overline{\mathbb{F}_q}$ -point $(x - x_0)$ of $\mathbb{A}_{\overline{\mathbb{F}_q}}^1$ for any $x_0, y_0 \in \overline{\mathbb{F}_q}$ such that $y_0^p - y_0 = g(x_0)$. Obviously, for any point x_0 , there is some $y_0 \in \overline{\mathbb{F}_q}$ such that the set $\pi^{-1}(x_0)$ is of the form

$$\{(x_0, y_0), (x_0, y_0 + 1), \dots, (x_0, y_0 + p - 1)\}.$$

Lemma 2.1. *Assume that $x_0 \in \mathbb{F}_{q^m}$. Then the number of \mathbb{F}_{q^m} -points in $\pi^{-1}(x_0)$ is*

$$\sum_{\chi} \chi(\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(g(x_0))),$$

where χ runs through all additive characters from \mathbb{F}_p to μ_p .

Proof. For any $a \in \mathbb{F}_p$, one can easily check that

$$\sum_{\chi} \chi(a) = \begin{cases} 0, & \text{if } a \neq 0; \\ p, & \text{if } a = 0. \end{cases}$$

Let (x_0, y_0) be a point in $\pi^{-1}(x_0)$. We only need to show that $y_0 \in \mathbb{F}_{q^m}$ if and only if $\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(g(x_0)) = 0$. This follows from the following exact sequence

$$0 \rightarrow \mathbb{F}_p \xrightarrow{\text{inc}} \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m} \xrightarrow{\text{Tr}} \mathbb{F}_p \rightarrow 0,$$

where the middle map is given by $a \mapsto a^p - a$. □

Proposition 2.2. $P_1(C(g), t) = \prod_{\chi \neq 1} L(g, \chi, t)$.

Proof. By Lemma 2.1,

$$S_m(U) = \sum_{x_0 \in \mathbb{F}_{q^m}} \sum_{\chi} \chi(\text{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_p}(g(x_0))) = q^m + \sum_{\chi \neq 1} S_m(g, \chi).$$

As $S_m(C(g)) = 1 + S_m(U)$ and $P_1(C(g), t) = (1 - t)(1 - qt)Z(C(g), t)$, by definition of Zeta functions,

$$P_1(C(g), t) = (1 - t)(1 - qt) \times \exp \left[\sum_{m=1}^{\infty} \left(1 + q^m + \sum_{\chi \neq 1} S_m(g, \chi) \right) \frac{t^m}{m} \right].$$

The Proposition follows from the definition of L -functions. □

For any polygon P , denote by $\text{Len}(P, \lambda)$ the length of the side of slope of λ . As the Newton polygon $\text{NP}_{\mathfrak{p}}(f)$ of $L(\overline{f}, \chi, t)$ does not depend on the choice of $\chi \neq 1$, we have the following result.

Corollary 2.3. *For any λ , $\text{Len}(\text{NP}_q^1(C(\overline{f})), \lambda) = (p-1)\text{Len}(\text{NP}_{\mathfrak{p}}(f), \lambda)$.*

Lemma 2.4. *Write $L(g, \chi, t)$ in the form $(1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{d-1} t)$. For any $m \geq 1$, we have*

$$S_m(g, \chi) = -(\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d-1}^m).$$

Proof. By definition of $L(g, \chi, t)$,

$$(1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{d-1} t) = \exp \left(\sum_{m=1}^{\infty} S_m(g, \chi) \frac{t^m}{m} \right).$$

Taking logarithm and expanding both sides, we can get the formula by comparing the coefficients of t^m on both sides. \square

Lemma 2.5. *Write $L(g, \chi, t)$ in the form $(1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{d-1} t)$. For any $n \geq 1$, we have*

$$L(g/\mathbb{F}_{q^n}, \chi, t) = (1 - \alpha_1^n t)(1 - \alpha_2^n t) \cdots (1 - \alpha_{d-1}^n t).$$

In particular, the q -adic Newton polygon of $L(g, \chi, t)$ is the same as the q^n -adic Newton polygon of $L(g/\mathbb{F}_{q^n}, \chi, t)$.

Proof. Assume that $L(g/\mathbb{F}_{q^n}, \chi, t) = (1 - \beta_1 t)(1 - \beta_2 t) \cdots (1 - \beta_{d-1} t)$. It is clear that

$$S_m(g/\mathbb{F}_{q^n}, \chi) = S_{mn}(g, \chi)$$

holds for any $m \geq 0$. By Lemma 2.4, we have

$$\beta_1^m + \beta_2^m + \cdots + \beta_{d-1}^m = \alpha_1^{mn} + \alpha_2^{mn} + \cdots + \alpha_{d-1}^{mn}.$$

Hence we have

$$\sum_{m=0}^{\infty} (\beta_1^m + \beta_2^m + \cdots + \beta_{d-1}^m) t^m = \sum_{m=0}^{\infty} (\alpha_1^{mn} + \alpha_2^{mn} + \cdots + \alpha_{d-1}^{mn}) t^m$$

That is

$$\frac{1}{1 - \beta_1 t} + \frac{1}{1 - \beta_2 t} + \cdots + \frac{1}{1 - \beta_{d-1} t} = \frac{1}{1 - \alpha_1^n t} + \frac{1}{1 - \alpha_2^n t} + \cdots + \frac{1}{1 - \alpha_{d-1}^n t}.$$

Comparing the poles on both sides, we are done. \square

Proposition 2.6. *Let L/K be a finite extension of number fields and \mathfrak{P} a place of L above \mathfrak{p} a place of K . Then*

$$\text{NP}_{\mathfrak{p}}(f) = \text{NP}_{\mathfrak{P}}(f).$$

In particular, $\lim_{\mathfrak{p} \in \Sigma_K} \text{NP}_{\mathfrak{p}}(f)$ exists if and only if $\lim_{\mathfrak{P} \in \Sigma_L} \text{NP}_{\mathfrak{P}}(f)$ exists

Proof. By definition, $\text{NP}_{\mathfrak{p}}(f)$ is the q -adic Newton polygon of $L(\overline{f}/k_{\mathfrak{p}}, \chi, t)$ and $\text{NP}_{\mathfrak{P}}(f)$ is the $q^{[k_{\mathfrak{P}}:k_{\mathfrak{p}}]}$ -adic Newton polygon of $L(\overline{f}/k_{\mathfrak{P}}, \chi, t)$. By Lemma 2.5, we have $\text{NP}_{\mathfrak{p}}(f) = \text{NP}_{\mathfrak{P}}(f)$. \square

3. DIVISIBILITY RELATIONS OF ZETA FUNCTIONS

We fix p , h and $q = p^h$ as in the previous section. Let X, Y be two smooth separated algebraic varieties over \mathbb{F}_q . Let $\pi : Y \rightarrow X$ be an \mathbb{F}_q -morphism and \mathcal{F} be a sheaf over the étale site \overline{X}_{et} , where $\overline{X} = X_{\mathbb{F}_q}$. The morphism $\pi_{\mathbb{F}_q}$ induces a map $\pi^* : H_c^r(\overline{X}_{et}, \mathcal{F}) \rightarrow H_c^r(\overline{Y}_{et}, \pi^* \mathcal{F})$. If π is an étale morphism, then there is a natural isomorphism $H_c^r(\overline{Y}_{et}, \pi^* \mathcal{F}) \xrightarrow{\text{can}} H_c^r(\overline{X}_{et}, \pi_* \pi^* \mathcal{F})$.

Lemma 3.1. *Suppose that $\pi : Y \rightarrow X$ is a finite étale \mathbb{F}_q -morphism of degree δ . Then there is a trace map $\text{tr} : \pi_* \pi^* \mathcal{F} \rightarrow \mathcal{F}$ such that*

$$\text{tr} \circ \text{can} \circ \pi^* = \delta.$$

In particular, if δ is invertible on \mathcal{F} , then π^ is injective.*

Proof. See pages 168-171 in [8]. □

By the Grothendieck-Lefschetz trace formula (see [6]), the number N_s of \mathbb{F}_{q^s} -rational points on X is

$$N_s = \sum_{i=0}^{2d} (-1)^i \text{Tr}((F^*)^s, H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell)),$$

where F is the Frobenius endomorphism on X/\mathbb{F}_q . So the Zeta function on X is

$$Z(X, t) = \frac{P_1(X, t) P_3(X, t) \cdots P_{2d-1}(X, t)}{P_0(X, t) P_2(X, t) \cdots P_{2d}(X, t)}$$

with $P_i(X, t) = \det(1 - tF^* \mid H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell))$.

Theorem 3.2. *If there is some finite étale morphism $\pi : Y \rightarrow X$, then*

$$P_i(X, t) \mid P_i(Y, t).$$

Proof. As F commutes with π , we have the following commutative diagram

$$\begin{array}{ccc} H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell) & \xrightarrow{\pi^*} & H_c^i(\overline{Y}_{et}, \mathbb{Q}_\ell) \\ \downarrow F^* & & \downarrow F^* \\ H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell) & \xrightarrow{\pi^*} & H_c^i(\overline{Y}_{et}, \mathbb{Q}_\ell). \end{array}$$

By Lemma 3.1, π^* is injective. The commutative diagram implies that $H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell)$ can be viewed as an invariant subspace of $H_c^i(\overline{Y}_{et}, \mathbb{Q}_\ell)$ under the action of F^* . So we have

$$\det(1 - tF^* \mid H_c^i(\overline{X}_{et}, \mathbb{Q}_\ell)) \mid \det(1 - tF^* \mid H_c^i(\overline{Y}_{et}, \mathbb{Q}_\ell)). \quad \square$$

Corollary 3.3. *Let X, Y be two smooth complete curves over \mathbb{F}_q . If there is some finite \mathbb{F}_q -morphism $\pi : Y \rightarrow X$, then*

$$P_1(X, t) \mid P_1(Y, t).$$

Proof. By removing the compositions of Frobenius on X , we can assume that π is unramified at the generic point. Let $U \subsetneq X$ be a nonempty open subvariety of X such that the base change $\pi : Y_U \rightarrow U$ is a finite étale morphism. Denote by Z the complement of U in X , of which the closed points are finite. By the definition of Zeta function, we have

$$Z(X, t) = Z(U, t) \times \prod_x \frac{1}{1 - t^{\deg x}}$$

and

$$Z(Y, t) = Z(Y_U, t) \times \prod_y \frac{1}{1 - t^{\deg y}},$$

where x (resp. y) runs through all prime \mathbb{F}_q -rational 0-cycles on Z (resp. Y_Z) à la Monsky. As X, Y are complete curves,

$$Z(X, t) = \frac{P_1(X, t)}{(1 - t)(1 - qt)}, \quad Z(Y, t) = \frac{P_1(Y, t)}{(1 - t)(1 - qt)}.$$

As U, Y_U are not complete, we have

$$Z(U, t) = \frac{P_1(U, t)}{1 - qt}, \quad Z(Y_U, t) = \frac{P_1(Y_U, t)}{1 - qt}.$$

By Theorem 3.2, $P_1(U, t) \mid P_1(Y_U, t)$. So from the above formulas, we have

$$P_1(X, t) \frac{\prod_x (1 - t^{\deg x})}{1 - t} \mid P_1(Y, t) \frac{\prod_y (1 - t^{\deg y})}{1 - t}.$$

Weil's conjecture tells us that the complex absolute values of all roots of $P_1(X, t)$ and $P_1(Y, t)$ are $q^{-\frac{1}{2}}$. We are done. \square

4. GLOBAL PERMUTATION POLYNOMIALS AND DICKSON POLYNOMIALS

Let a be an element in a commutative ring R . For any $n \geq 1$, the Dickson polynomial of the first kind associated to a of degree n , denote by $D_n(x, a)$, is the unique polynomial over R such that

$$D_n\left(x + \frac{a}{x}, a\right) = x^n + \frac{a^n}{x^n}. \quad (4.1)$$

One can easily check that

$$D_n(x, 0) = x^n \quad (4.2)$$

and

$$D_{mn}(x, a) = D_m(D_n(x, a), a^n). \quad (4.3)$$

Lemma 4.1. *Let $a \in \mathbb{F}_q$ and n be a positive integer.*

1). *If $a = 0$, then $D_n(x, 0) = x^n$ is a permutation polynomial of \mathbb{F}_q if and only if $(n, q - 1) = 1$.*

2). *If $a \neq 0$, then $D_n(x, a)$ is a permutation polynomial of \mathbb{F}_q if and only if $(n, q^2 - 1) = 1$.*

Proof. Due to [4], see [7, Theorem 7.16] for quick reference. \square

Proposition 4.2 (Fried-Turnwald). *Let f be a GPP over K . Then f is a composition of linear polynomials $\alpha_i x + \beta_i \in K[x]$ and the Dickson polynomials $D_{n_j}(x, a_j)$, where $a_j \in K$ and n_j are positive integers.*

Proof. See [5, Theorem 2] or [10, Theorem 2]. \square

5. PROOF OF MAIN RESULT

We call an element (\mathfrak{p}, a, n) in $\Sigma_K \times K \times \mathbb{Z}_{>1}$ an *admissible triple* if $a \in \mathcal{O}_{\mathfrak{p}}$, $\mathfrak{p} \nmid 3n\omega$ and the Dickson polynomial $D_n(x, \bar{a})$ is a permutation polynomial on $k_{\mathfrak{p}}$, where ω is the number of the roots of unity in K .

Lemma 5.1. *If (\mathfrak{p}, a, n) is an admissible triple, then $(n, \omega) = 1$. In particular, $2 \nmid n$. Moreover if $a \neq 0$, then $3 \nmid n$.*

Proof. As $D_n(x, \bar{a})$ is a permutation polynomial on $k_{\mathfrak{p}}$, by Lemma 4.1, $(n, q-1) = 1$. As $\mathfrak{p} \nmid \omega$, the reduction induces an inclusion $\mu_K \subset \mu_{k_{\mathfrak{p}}}$, and hence $\omega \mid q-1$. So we have $(n, \omega) = 1$.

If $a \neq 0$, by Lemma 4.1, $(n, q^2-1) = 1$. As $3 \mid q^2-1$, so we have $3 \nmid n$. \square

Proposition 5.2. *Suppose that f contains $D_n(x, a)$ as a composition factor. Then for $\mathfrak{p} \in \Sigma_K(f)$ such that (\mathfrak{p}, a, n) is an admissible triple, there exists $v_0 \in \mathbb{Q}$ such that $\text{Len}(\text{NP}_{\mathfrak{p}}(f), v_0) \geq 2$ and hence the gap between $\text{NP}_{\mathfrak{p}}(f)$ and $\text{HP}(f)$ is at least $\frac{1}{2d}$.*

Proof. Write f in the form $f_1 \circ D_n(x, a) \circ f_3$. By (4.3) and Lemma 5.1, we can assume that n is an odd prime number. For any positive integer m , denote by $k_{\mathfrak{p}}^m$ the unique extension of $k_{\mathfrak{p}}$ of degree m . Set $e = 1$ if $\bar{a} = 0$ and otherwise $e = 2$. By Lemma 4.1, we have $(q^e - 1, n) = 1$. As n is an odd prime number, $(q^{(n-1)s+1})^e \equiv q^e \not\equiv 1 \pmod{n}$ and so $((q^{(n-1)s+1})^e - 1, n) = 1$. Using Lemma 4.1 again, $D_n(x, \bar{a})$ is permutation polynomial of $k_{\mathfrak{p}}^m$, where $m = (n-1)s+1$ and s is a non-negative integer. For these m and any nontrivial character $\chi : \mathbb{F}_p \rightarrow \mu_p$, we have that

$$S_m(\bar{f}_1, \chi) = S_m(\bar{f}_1 \circ D_n(x, \bar{a}), \chi). \quad (5.1)$$

Assume that

$$L(\bar{f}_1, \chi, t) = (1 - \alpha_1 t)(1 - \alpha_2 t) \cdots (1 - \alpha_{d_1-1} t)$$

and

$$L(\bar{f}_1 \circ D_n(x, \bar{a}), \chi, t) = (1 - \beta_1 t)(1 - \beta_2 t) \cdots (1 - \beta_{nd_1-1} t),$$

where d_1 is the degree of f_1 . Lemma 2.4 implies that

$$S_m(\bar{f}_1, \chi) = -(\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d_1-1}^m)$$

and

$$S_m(\bar{f}_1 \circ D_n(x, \bar{a}), \chi) = -(\beta_1^m + \beta_2^m + \cdots + \beta_{nd_1-1}^m).$$

By (5.1), we have an equality of power series

$$\sum_{m=(n-1)s+1} (\alpha_1^m + \alpha_2^m + \cdots + \alpha_{d_1-1}^m) t^m = \sum_{m=(n-1)s+1} (\beta_1^m + \beta_2^m + \cdots + \beta_{nd_1-1}^m) t^m.$$

Hence

$$\sum_{i=1}^{d_1-1} \frac{\alpha_i t}{1 - (\alpha_i t)^{n-1}} = \sum_{i=1}^{nd_1-1} \frac{\beta_i t}{1 - (\beta_i t)^{n-1}}.$$

Comparing the poles on both sides, there exist $1 \leq i < j \leq nd_1 - 1$ such that

$$\beta_i^{n-1} = \beta_j^{n-1}.$$

Denote by v_0 the q -adic valuation of β_i (and of β_j). Then

$$\text{Len}(\text{NP}_{\mathfrak{p}}(f_1 \circ D_n(x, a)), v_0) \geq 2.$$

Denote $C' = C(\overline{f_1} \circ D_n(x, \overline{a}))$, by Corollary 2.3,

$$\text{Len}(\text{NP}_q^1(C'), v_0) \geq 2(p-1).$$

Denote $C = C(f)$, one can check that

$$k_{\mathfrak{p}}(C') = k_{\mathfrak{p}}(x, y') \text{ and } k_{\mathfrak{p}}(C) = k_{\mathfrak{p}}(x, y),$$

where $(y')^p - y' = \overline{f_1} \circ D_n(x, \overline{a})$ and $y^p - y = f(x)$. The embedding

$$k_{\mathfrak{p}}(x, y') \rightarrow k_{\mathfrak{p}}(x, y)$$

sending x to $\overline{f_3}$ and y' to y induces a non-constant morphism

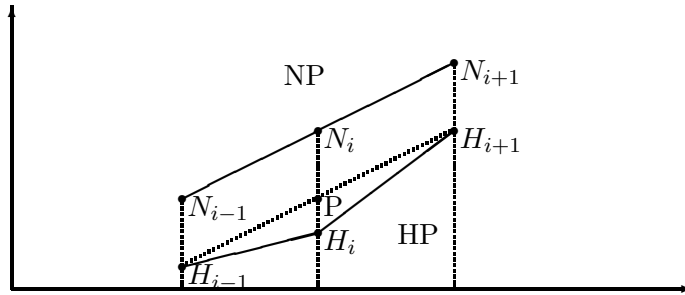
$$\pi : C \rightarrow C'$$

of complete smooth curves. By Proposition 3.3,

$$\text{Len}(\text{NP}_q^1(C), v_0) \geq \text{Len}(\text{NP}_q^1(C'), v_0) \geq 2(p-1).$$

Using Corollary 2.3 again, we have

$$\text{Len}(\text{NP}_{\mathfrak{p}}(f), v_0) \geq 2.$$



As in the above diagram, we assume that $N_{i-1}N_i$ and N_iN_{i+1} are of the same slope. The slopes of $H_{i-1}H_i$ and H_iH_{i+1} are $\frac{i}{d}$ and $\frac{i+1}{d}$, respectively. As the HP is below the NP, we know that N_{i+1} is above H_{i+1} . Hence the middle point N_i of $N_{i-1}N_{i+1}$ is above P that of $H_{i-1}H_{i+1}$. So we have

$$|N_i H_i| \geq |P H_i| \geq \frac{1}{2d}. \quad \square$$

Proof of Main Result. Write f in the form $f_1 \circ f_2 \circ f_3$, where f_2 is a GPP over K of degree > 1 . As every composition factor of a GPP is still a GPP, by Proposition 4.2, we can assume that $f_2 = D_n(x, a)$ is a GPP over K , where $a \in K$ and $n \in \mathbb{Z}_{>1}$.

By definition, there are infinitely many $\mathfrak{p} \in \Sigma_K$ such that (\mathfrak{p}, n, a) is an admissible triple. For those \mathfrak{p} , by Proposition 5.2, the gap between $NP_{\mathfrak{p}}(f)$ and $HP(f)$ is at least $\frac{1}{2d}$. However, for places \mathfrak{p} such that $p_{\mathfrak{p}} \equiv 1 \pmod{d}$, we know $NP_{\mathfrak{p}}(f) = HP(f)$. So the limit does not exist. \square

Acknowledgement. Research is partially supported by National Key Basic Research Program of China (Grant No. 2013CB834202) and National Natural Science Foundation of China (Grant No. 11171317 and 11571328).

REFERENCES

- [1] A. Adolphson, S. Sperber, *Newton polyhedra and the degree of the L-function associated to an exponential sum*, Invent. Math., 88(1987), 555-569.
- [2] A. Adolphson, S. Sperber, *Exponential sums and Newton polyhedra: Cohomology and estimates*, Ann. of Math., 130(1989), 367-406.
- [3] R. Blache, E. Férard, H.J. Zhu, *Hodge-Stickelberger polygons for L-functions of exponential sums of $P(x^s)$* , Math. Res. Lett. 15 (2008), no. 5, 1053-1071.
- [4] L. E. Dickson, *The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group*. Ann. of Math. 11 (1896/97), no. 1-6, 65120, 161183.
- [5] M. Fried, *On a conjecture of Schur*. Michigan Math. J. 17(1970), 41-55.
- [6] A. Grothendieck, *Séminaire de Géométrie Algébrique du Bois Marie - 1965-66 - Cohomologie l-adique et Fonctions L - (SGA 5)*, Lecture Notes in Mathematics 589, Springer, 1977.
- [7] R. Lidl, H. Niederreiter, *Finite fields*. Encyclopedia of Mathematics and its Applications, 20. Addison-Wesley Publishing Company, Reading, MA, 1983.
- [8] J. S. Milne, *Étale cohomology*, Princeton Mathematical Series, 33. Princeton University Press, Princeton, N.J., 1980.
- [9] I. Schur, *Über den Zusammenhang zwischen einem Problem der Zahlentheorie und einem Satz über algebraische Funktionen*. S.-B. Preuss. Akad. Wiss. Berlin(1923), 123-134.
- [10] G. Turnwald, *On Schur's Conjecture*. J. Austral. Math. Soc. Ser. A 58 (1995), no. 3, 312-357.
- [11] A. Weil, *Numbers of solutions of equations in finite fields*. Bull. Amer. Math. Soc. 55 (1949). 497-508.
- [12] R. Yang, *Newton polygons of L-functions of polynomials of the form $x^d + \lambda x$* , Finite Fields Appl. 9 (2003), no. 1, 59-88.

WU WEN-TSUN KEY LABORATORY OF MATHEMATICS, SCHOOL OF MATHEMATICAL SCIENCES, UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA, HEFEI, ANHUI 230026, P. R. CHINA

E-mail address: yiouyang@ustc.edu.cn, yjb@mail.ustc.edu.cn